REMARKS

General Remarks

In the current and non-final Office Action, claims 1-47 were examined.

Generally, claims 1-47 were rejected.

Specifically:

Claims 1-2, 4-11, 13-28, 30-31, 33-35, and 37-42 were "rejected under 35 U.S.C. 102(e) as being anticipated by Downs et al (US 6,574,609)."

Claims 3, 12, 29, 32, 36, and 43-47 were "rejected under 35 U.S.C. 103(a) as being unpatentable over Downs et al. (US 6,574,609) as applied to claims 1-2, 4-11, 13-28, 30-31, 33-35, and 37-42 above, and further in view of Yoshida et al. (US 6,674,874)."

It is respectfully submitted that the rejections are inappropriate and unsupportable under both the facts and the law.

This "Remarks" section is divided into two additional subsections entitled: "Response to Office Action Assertions as to the Non-persuasiveness of Applicant's Arguments" and "Arguments for Patentability".

Of claims 1-47, there are seven (7) independent claims 1, 11, 17, 25, 30, 35, and 43. They are addressed below.

Response to Office Action Assertions

as to the Non-persuasiveness of Applicant's Arguments

On pages 2-4 at paragraph #1 the current Office Action reads: "Thc applicant's arguments filed March 15, 2005 havc been fully considered but they are not persuasive."

The respective independent claims 1, 11, 17, 25, 30, 35, and 43 are individually addressed in the respective subparagraphs a, b, c, d, e, f, and g of paragraph #1 of the current Office Action.

Subparagraph a. of the current Office Action is directed to claim 1 and reads as follows:

> a. The applicant argues that the prior art does not teach Claim 1: an authentication module configured to access a certificate, which indicates permissible uses of the digital content file, associated with and separate from thc digital content file. The examiner disagrees. Downs teachcs an authentication module configured to access a certificate, which indicates permissible uses of the digital content file, associated with and separate from the digital content file (column 10, lines 43-50)

Downs et al. at column 10, lines 43-50 rcads:

> Once an Electronic Digital Content Store(s) 103 completes a valid request for electronic Content 113 from an End-User(s), the Electronic Digital Content Store(s) 103 is responsible for authorizing the Clearinghouse(s) 105 to release the decryption key for the Content 113 to the customer. The Elcctronic Digital Content

> Store(s) also authorizes the download of the SC containing the Content 113. The Electronic Digital Content Store(s) may elect to ...

It is respectfully submitted that the above-quoted portion of Downs et al. fails to describe and/or teach at least **a certificate, which indicates permissible uses of the digital content file,** as recited in claim 1.

Subparagraph b. of the current Office Action is directed to claim 11 and reads as follows:

> b. The applicant argues that the prior art does not teach Claim 11: associating the digital content file with a certificate that contains copyright information including at least one indication regarding a permissible use of the digital content file and is not a part of the digital content file. The examiner disagrees. Downs teaches associating the digital content file with a certificate that contains copyright information including at least one indication regarding a permissible use of the digital content file and is not a part of the digital content file (column 46, lines 17-43).

Downs et al. at column 46, lines 17-43 reads:

> The Secure Digital Content Electronic Distribution System 100 provides the ability to handle retransmissions of Content 113. This is typically performed by a Customer Service Interface 184. Electronic Digital Content Store(s) 103 provides a user interface that the End-User(s) can step through in order to initiate a retransmission. The End-User(s) goes to the Electronic Digital Content Store(s) 103 site where the Content 113 item was purchased in order to request a retransmission of the Content 113.
>
> Retransmissions of Content 113 are done when an End-User(s) requests a new copy of a previously purchased Content 113 item because the Content 113 could not be downloaded or the Content 113 that was downloaded is not usable. The Electronic Digital Content Store(s) 103 determines whether the End-User(s) is entitled to do a retransmission of the Content 113. If the End-User(s) is entitled to a retransmission, then the Electronic Digital Content Store(s) 103 builds a

> Transaction SC(s) 640 that includes the Offer SC(s) 641 of the Content 113 item(s) being retransmitted. The Transaction SC(s) 640 is sent to the End-User Devicc(s) 109 and the identical steps as for a purchase transaction are performed by the End-User(s). If the End-User Device(s) 109 has a scrambled key(s) in the key library for the Content 113 item(s) undergoing retransmission, then the Transaction SC(s) 640 includes information that instructs the End-User Device(s) 109 to delete the scrambled key(s).

It is respectfully submitted that the above-quoted portion of Downs et al. fails to describe and/or teach at least **a certificate that contains copyright information including at least one indication regarding a permissible use of the digital content file** as recited in claim 11.

Subparagraph c. of the current Office Action is directed to claim 17 and reads as follows:

> c. The applicant argues that the prior art does not teach Claim 17: configuring the certificate file with permissible use information about the digital content file so that when the digital content file is processed, the digital content file is processed in accordance with the permissible use information contained in the certificate file. The examiner disagrees. Downs teaches configuring the certificate file with permissible use information about the digital content file so that when the digital content file is processed, the digital content file is processed in accordance with the permissible use information contained in the certificate file (column 10, lines 43-50)

Downs et al. at column 10, lines 43-50 reads:

> Once an Electronic Digital Content Store(s) 103 completes a valid request for electronic Content 113 from an End-User(s), the Electronic Digital Content Store(s) 103 is responsible for authorizing the Clearinghouse(s) 105 to release the decryption key for the Content 113 to the customer. The Electronic Digital Content Store(s) also authorizes the download of the SC containing the Content 113. The Electronic Digital Content Store(s) may elect to ...

It is respectfully submitted that the above-quoted portion of Downs et al. fails to describe and/or teach at least **configuring the certificate file with permissible use information about the digital content file** as recited in claim 17.

Subparagraph d. of the current Office Action is directed to claim 25 and reads as follows:

> d. The applicant argues that the prior art does not teach Claim 25: if the watermark signal is detected, attempting to locate a certificate associated with the digital content file, the certificate including copyright information having at least one indication regarding a permissible use of the digital content file. The examiner disagrees. Downs teaches if the watermark signal is detected, attempting to locate a certificate associated with the digital content file, the certificate including copyright information having at least one indication regarding a permissible use of the digital content file (column 46, lines 17-43).

Downs et al. at column 46, lines 17-43 reads:

> The Secure Digital Content Electronic Distribution System 100 provides the ability to handle retransmissions of Content 113. This is typically performed by a Customer Service Interface 184. Electronic Digital Content Store(s) 103 provides a user interface that the End-User(s) can step through in order to initiate a retransmission. The End-User(s) goes to the Electronic Digital Content Store(s) 103 site where the Content 113 item was purchased in order to request a retransmission of the Content 113.
>
> Retransmissions of Content 113 are done when an End-User(s) requests a new copy of a previously purchased Content 113 item because the Content 113 could not be downloaded or the Content 113 that was downloaded is not usable. The Electronic Digital Content Store(s) 103 determines whether the End-User(s) is entitled to do a retransmission of the Content 113. If the End-User(s) is entitled to a retransmission, then the Electronic Digital Content Store(s) 103 builds a Transaction SC(s) 640 that includes the Offer SC(s) 641 of the Content 113 item(s) being retransmitted. The Transaction SC(s) 640 is sent to the End-User Device(s)

> 109 and the identical steps as for a purchase transaction are performed by the End-User(s). If the End-User Device(s) 109 has a scrambled key(s) in the key library for the Content 113 item(s) undergoing retransmission, then the Transaction SC(s) 640 includes information that instructs the End-User Device(s) 109 to delete the scrambled key(s).

It is respectfully submitted that the above-quoted portion of Downs et al. fails to describe and/or teach at least **the certificate including copyright information having at least one indication regarding a permissible use of the digital content file** as recited in claim 25.

Subparagraph e. of the current Office Action is directed to claim 30 and reads as follows:

> e. The applicant argues that the prior art does not teach Claim 30: the certificate containing copyright information including at least one indication regarding a permissible use of the digital content file. The examiner disagrees. Downs teaches the certificate containing copyright information including at least one indication regarding a permissible use of the digital content file (column 46, lines 17-43).

Downs et al. at column 46, lines 17-43 reads:

> The Secure Digital Content Electronic Distribution System 100 provides the ability to handle retransmissions of Content 113. This is typically performed by a Customer Service Interface 184. Electronic Digital Content Store(s) 103 provides a user interface that the End-User(s) can step through in order to initiate a retransmission. The End-User(s) goes to the Electronic Digital Content Store(s) 103 site where the Content 113 item was purchased in order to request a retransmission of the Content 113.
>
> Retransmissions of Content 113 are done when an End-User(s) requests a new copy of a previously purchased Content 113 item because the Content 113 could not be downloaded or the Content 113 that was downloaded is not usable. The Electronic Digital Content Store(s) 103 determines whether the End-User(s) is

> entitled to do a retransmission of the Content 113. If the End-User(s) is entitled to a retransmission, then the Electronic Digital Content Store(s) 103 builds a Transaction SC(s) 640 that includes the Offer SC(s) 641 of the Content 113 item(s) being retransmitted. The Transaction SC(s) 640 is sent to the End-User Device(s) 109 and the identical steps as for a purchase transaction are performed by the End-User(s). If the End-User Device(s) 109 has a scrambled key(s) in the key library for the Content 113 item(s) undergoing retransmission, then the Transaction SC(s) 640 includes information that instructs the End-User Device(s) 109 to delete the scrambled key(s).

It is respectfully submitted that the above-quoted portion of Downs et al. fails to describe and/or teach at least **the certificate containing copyright information including at least one indication regarding a permissible use of the digital content file** as recited in claim 30.

Subparagraph f. of the current Office Action is directed to claim 35 and reads as follows:

> f. The applicant argues that the prior art does not teach Claim 35: if the watermark is detected, attempting to locate a certificate that is associated with the digital content file, the certificate containing instructions regarding the digital content file . . . wherein the watermark only indicates the existence of the certificate. The examiner disagrees. Downs teaches if the watermark is detected, attempting to locate a certificate that is associated with the digital content file, the certificate containing instructions regarding the digital content file . . . wherein the watermark only indicates the existence of the certificate (column 10, lines 43-50 and column 7, line 35-column 8, line 29).

Downs et al. at column 10, lines 43-50 reads:

> Once an Electronic Digital Content Store(s) 103 completes a valid request for electronic Content 113 from an End-User(s), the Electronic Digital Content Store(s) 103 is responsible for authorizing the Clearinghouse(s) 105 to release the decryption key for the Content 113 to the customer. The Electronic Digital Content

Store(s) also authorizes the download of the SC containing the Content 113. The Electronic Digital Content Store(s) may elect to ...

Downs et al. at column 7, line 35 to column 8, line 29 reads:

Licensing authorization and control are implemented through the use of a Clearinghouse(s) entity and Secure Container (SC) technology. The Clearinghouse(s) provides licensing authorization by enabling intermediate or End-User(s) to unlock content after verification of a successful completion of a licensing transaction. Secure Containers are used to distribute encrypted content and information among the system components. A SC is a cryptographic carrier of information or content that uses encryption, digital signatures, and digital certificates to provide protection against unauthorized interception or modification of electronic information and content. It also allows for the verification of the authenticity and integrity of the Digital Content. The advantage of these rights management functions is that the electronic Digital Content distribution infrastructure does not have to be secure or trusted. Therefore transmission over network infrastructures such as the Web and Internet. This is due to the fact that the Content is encrypted within Secure Containers and its storage and distribution are separate from the control of its unlocking and use. Only users who have decryption keys can unlock the encrypted Content, and the Clearinghouse(s) releases decryption keys only for authorized and appropriate usage requests. The Clearinghouse(s) will not clear bogus requests from unknown or unauthorized parties or requests that do not comply with the content's usage conditions as set by the content proprietors. In addition, if the SC is tampered with during its transmission, the software in the Clearinghouse(s) determines that the Content in a SC is corrupted or falsified and repudiate the transaction.

The control of Content usage is enabled through the End-User Player Application 195 running on an End-User Device(s). The application embeds a digital code in every copy of the Content that defines the allowable number of secondary copies and play backs. Digital watermarking technology is used to generate the digital code, to keep it hidden from other End-User Player Application 195, and to make it resistant to alteration attempts. *When the Digital Content is accessed in a compliant End-User Device(s), the End-User Player Application 195 reads the watermark to check the use restrictions and updates the watermark as*

> *required.* If the requested use of the content does not comply with the usage conditions, e.g., the number of copies has been exhausted, the End-User Device(s) will not perform the request.
>
> *Digital watermarking also provides the means to identify the origin of authorized or unauthorized copies of Content. An initial watermark in the Content is embedded by the content proprietor to identify the content proprietor, specify copyright information, define geographic distribution areas, and add other pertinent information. A second watermark is embedded in the Content at the End-User Device(s) to identify the content purchaser (or licensee) and End-User Device(s), specify the purchase or license conditions and date, and add any other pertinent information.*
>
> Since watermarks become an integral part of the Content, they are carried in the copies independent of whether the copies were authorized or not. Thus the Digital Content always contains information regarding its source and its permitted use regardless of where the content resides or where it comes from. This information may be used to combat illegal use of the Content.
>
> (*italicized emphasis above added by Applicant's representative*)

It is respectfully submitted that the above-quoted portions of Downs et al. fail to describe and/or teach at least **the certificate containing instructions regarding the digital content file** [and] **wherein the watermark only indicates the existence of the certificate** as recited in claim 35. Furthermore, it is respectfully submitted that especially the italicized parts actually teach away from **wherein the watermark only indicates the existence of the certificate** as recited in claim 35.

<u>Subparagraph g.</u> of the current Office Action is directed to claim 43 and reads as follows:

> g. The applicant argues that the prior art does not teach Claim 43: wherein the 1-bit watermark indicatez the presence of a certificate associated with the digital content, the certificate containing copyright information including at least one indication regarding a permissible use of the digital content and being stored

apart from the digital content. The examiner disagrees. Downs teaches wherein the 1-bit watermark indicates the presence of a certificate associated with the digital content, the certificate containing copyright information including at least one indication regarding a permissible use of the digital content and being stored apart from the digital content. Downs discloses digital watermarks being embedded in digital content file without specific details regarding 1-bit watermark. In the same field of endeavor, however, Yoshida discloses a digital watermark embedding system comprising the step of embedding 1-bit watermark (column 1, lines 38-52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to embed 1-bit watermark as taught by Yoshida in the system of Downs because it provides a digital watermark technique for integratedly managing a plurality of kinds of contents such as still images, motion images, audio, sound.

Yoshida et al. at column 1, lines 38-52 reads:

> According to a method of using the Fourier transformation, a PN line is added to input contents and the resultant contents are diffused and, thereafter, divided into blocks. The Fourier transformation is performed every block and digital watermark information of 1 bit is embedded into one block. A reverse Fourier transformation is performed to the block in which the digital watermark information was embedded and the same PN line as that used at the first stage is again added to the resultant contents, so that the contents in which the digital watermark was embedded is derived. A detailed technique of the above method has been disclosed in, for example, Onishi, Oka, and Matsui, "Method of Watermark Signature into Image by PN line", Records of Symposium about Encryption and Information Security, SCIS 97-26B, 1997.

It is respectfully submitted that Downs et al. and/or Yoshida et al., including the above-quoted portions of both, fail to individually or jointly describe and/or teach at least **wherein the 1-bit watermark indicates the presence of a certificate associated with the digital content, the certificate containing copyright information including at least one indication regarding a permissible use of the digital content** as recited in claim 43.

Although Yoshida et al. does appear to mention the existence of a 1-bit digital watermark, there are at least two deficiencies with asserting that a combination of Downs et al. and Yoshida et al. renders claim 43 obvious, even assuming, *arguendo*, that any such combination is possible. First, there is no teaching in either reference as to how to use such a 1-bit watermark with the secure electronic content management system of Downs et al. In other words, there is no motivation (or at best insufficient motivation) to combine the two references and/or to modify Downs et al. such that the claimed invention taken as a whole is rendered obvious.

Second, Downs et al. actually teaches against using a 1-bit digital watermark inasmuch as the watermarks of Downs et al. are expressly intended to perform a number of functions in accordance with their intended purpose. For example, as reproduced above with regard to subparagraph f., "An initial watermark in the Content is embedded by the content proprietor to identify the content proprietor, specify copyright information, define geographic distribution areas, and add other pertinent information. A second watermark is embedded in the Content at the End-User Device(s) to identify the content purchaser (or licensee) and End-User Device(s), specify the purchase or license conditions and date, and add any other pertinent information." (Downs et al., Column 8, Lines 13-22.) Thus, the functions and purposes of watermarking in Downs et al. are destroyed and/or rendered inoperable by substituting the 1-bit watermark that is mentioned in Yoshida et al.

Consequently, in light of the above responses, it is respectfully submitted that the independent claims 1, 11, 17, 25, 30, 35, and 43 are allowable over the art and rejections of record.

Arguments for Patentability

I. It is respectfully submitted that no art of record (including Downs et al. and/or Yoshida et al.), either alone or in any combination, anticipates or renders obvious claims 1-43.

A. For example, (i) the secure container (SC) of Downs et al. includes usage conditions, *but* (ii) the certificate of Downs et al. does not include any such usage conditions.

It is respectfully noted that the current Office Action does not appear to have cited to any portion(s) of Downs et al. (or Yoshida et al.) that contradict the statements in the following paragraph.

The usage conditions of Downs et al. are separate from the certificate(s) of Downs et al. as indicated by the portions of Downs et al. that are cited and quoted below:

1. Downs et al. reads at column 15, lines 21-24, in pertinent part:

> "And Usage Conditions 206 for content licensing management as described below. *The SC(s) 200 comprises Usage Conditions 206...*"

(emphasis added)

2. Downs et al. reads at column 11, line 64 to column 12, line 9, in pertinent part:

> "The End-User Device(s) 109 manages the download and storage ofthe SCs containing the Digital Content; requests and manages receipt of the encrypted Digital Content keys from the Clearinghouse(s) 105; processes the watermark(s) every time the Digital Content is copied or played; manages the number of copies made (or deletion of the copy) in accordance with the Digital Content's Usage Conditions; and performs the copy to an external media or portable consumer device if permitted. The portable consumer device can perform a subset of the End-User Player Application 195 functions *in order to process the content's Usage Conditions embedded in the watermark.*"

(emphasis added)

3. Downs et al. reads at column 14, lines 41-49, in pertinent part:

> "A digital certificate is used to authenticate or verify the identity of a person or entity that has sent a digitally signed message. A certificate is a digital document issued by a certification authority that binds a public key to a person or entity. The certificate includes the public key, the name of the person or entity, an expiration date, the namne of the certification authority, and other information. The certificate also contains the digital signature of the certification authority."

4. Downs et al. reads at column 28, line 63 to column 29, line 12, in pertinent part:

> "Clearinghouse(s) Certificate(s)--A certificate from a certification authority or from the Clearinghouse(s) 105 that contains the signed Public Key 621 of the Clearinghouse(s) 105. There may be more than one certificate, in which case a hierarchical level structure is used with the

highest level certificate containing the public key to open the next lowest level certificate is reached which contains the Public Key 621 of the Clearinghouse(s) 105.

Certificate(s)–A certificate from a certification authority or from the Clearinghouse(s) 105 that contains the signed Public Key 621 of the entity that created the SC(s). There may be more than one certificate, in which case a hierarchical level structure is used with the highest level certificate containing the public key to open the next level certificate, and so on, until the lowest level certificate is reached which contains the public key of the SC(s) creator."

5. Downs et al. reads at column 11, lines 18-24, in pertinent part:

"Once these verifications are satisfied, the Clearinghouse(s) 105 sends the decryption key for the Content 113 to the requesting End-User(s) packed in a License SC. The key is encrypted in a manner so that only the authorized user can retrieve it. If the End-User's request is not verifiable, complete, or authorized, the Clearinghouse(s) 105 repudiates the request for the decryption key."

6. Downs et al. reads at column 28, lines 14-16, in pertinent part:

"Usage Conditions–A part that contains information that describes usage options, rules, and restrictions to be imposed on an End-User(s) for use of the Content 113."

7. Downs et al. reads at column 9, lines 51-62, in pertinent part:

"A Metadata Assimilation and Entry Tool 161 is used to extract metadata from the Content Provider(s)' Database 160 (for a music example the Content 113 information such as CD title, artist name, song title, CD artwork, and more) and to package it for electronic distribution. *The Metadata Assimilation and Entry Tool 161 is also used to enter the Usage Conditions for the Content 113.* The data in Usage Conditions can include copy restriction rules, the wholesale price, and any business rules deemed necessary. A Watermarking Tool is used to hide data in the Content 113 that identifies thc content owner, the processing date, and other relevant data."

(emphasis added)

8. Downs et al. reads at column 8, lines 13-29, in pertinent part:

"Digital watermarking also provides thc means to identify the origin of authorized or unauthorized copies of Content. An initial watermark in the Content is embedded by the content proprietor to identify the content proprietor, specify copyright information, define geographic distribution areas, and add other pertinent information. A second watermark is embedded in the Content at the End-User Device(s) to identify the content purchaser (or licensee) and End-User Device(s), specify the purchase or license conditions and datc, and add any other pertinent information.

Since watermarks become an integral part of the Content, they are carried in the copies independent of whether the copies were authorized or not. *Thus the Digital Content always contains information regarding its source and its permitted use regardless of where the content resides or where it comes from.* This information may be used to combat illegal use of the Content."

(emphasis added)

9. Downs et al. reads at column 20, lines 51-52, in pertinent part:

> "*The End-User Device(s) 109 uses a License Watermark 527 to embed the copy/play code within the Content 113.* Only the End-User Playcr Application 195 that is knowlcdgeable of the embedding algorithm and the associated scrambling key is able to read or modify the embedded data. The data is invisible or inaudible to a human observer; that is, the data introduces no perceivable degradation to the Content 113. Since the watermark survives several steps of content processing, data compression, D-to-A and A-to-D conversion, and signal degradation introduced by normal content handling, *the watermark stays with the Content 113 in any representation form, including analog representation.*"
>
> (emphasis added)

B. Thus, no art of record, either alone or in any combination, anticipates or renders obvious at least the following elements in conjunction with the other elements of their respective claims:

Claim 1: **an authentication module configured to access a certificate, which indicates permissible uses of the digital content file, associated with and separate from the digital content file ....**

Claim 11: **associating the digital content file with a certificate that contains copyright information including at least one indication regarding a permissible use of the digital content file and is not a part of the digital content file.**

Claim 17: **configuring the certificate file with permissible use information about the digital content file so that when the digital content file is processed, the digital content file is processed in accordance with the permissible use information contained in the certificate file.**

Claim 25: **if the watermark signal is detected, attempting to locate a certificate associated with the digital content file, the certificate including copyright information having at least one indication regarding a permissible use of the digital content file.**

Claim 30: **the certificate containing copyright information including at least one indication regarding a permissible use of the digital content file.**

Claim 35: **if the watermark is detected, attempting to locate a certificate that is associated with the digital content file, the certificate containing instructions regarding the digital content file . . . wherein the watermark only indicates the existence of the certificate.**

Claim 43: **wherein the 1-bit watermark indicates the presence of a certificate associated with the digital content, the certificate containing copyright information including at least one indication regarding a permissible use of the digital content and being stored apart from the digital content.**

Reasons for the allowability of independent claims 1, 11, 17, 25, 30, 35, and 43 have been provided above. Claims 2-10, 12-16, 18-24, 26-29, 31-34, 36-42, and 44-47 depend from these independent claims 1, 11, 17, 25, 30, 35, and 43, respectively. Although each also includes additional element(s) militating toward allowability, it is respectfully submitted that these dependent claims are allowable at least for the reasons given above in connection with their respective independent claims.

CONCLUSION

It is respectfully submitted that all of the pending claims 1-47 are allowable, and prompt action to that end is hereby requested.

Respectfully Submitted,

Date: 9/27/2005 By: Keith W. Saunders

Keith W. Saunders
Reg. No. 41,462
(509) 324-9256 x238